ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2016, T. 45, Nr. 4

An Advanced Elliptic Curve Cryptography based Mutual Authentication Scheme for Session Initiation Protocol

Yanrong Lu[1,2], Lixiang Li[1,2], Haipeng Peng[1,2], Yixian Yang[1,2]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, China*

[2] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications,China*

e-mail: li_lixiang2006@163.com

crossref http://dx.doi.org/10.5755/j01.itc.45.4.13401

Abstract. Session Initiation Protocol (SIP) as the controlling protocol has attracted much attention. SIP is one of the most widely used for securing and controlling communication over the Internet. Recently, Arshad and Ikram proposed an enhanced mutual authentication scheme for SIP based on Tasi's scheme. In this paper, we focus on the security weaknesses in the Arshad and Ikram's SIP authenticated scheme with Elliptic Curve Cryptography(ECC). We found that the enhanced scheme proposed by Arshad and Ikram was insecure against internal and masquerade attacks while not providing anonymity and update password phase. We then propose an advanced scheme to remedy the flaws and maintain benefits of the original scheme at the cost of increasing the computation consumptions slightly. Through a carefully security analysis and Burrows-Abadi-Needham (BAN) logic analysis of our scheme, we show that our scheme is more secure than other related schemes.

Keywords: authentication; elliptic curve cryptosystem; security; key agreement; session initiation protocol.

1. Introduction

Multimedia service is one of the most important application classes of wired or wireless networks. The session initiation protocol (SIP) is a great importance protocol and has been widely used for multimedia services. SIP [1-3] is a text based and one of the most popular client/sever protocols for multimedia services. Authentication is a necessary process when a remote user wants to get services from the corresponding sever [4-8]. Most communication environments of SIP are unsafe which naturally raises the issue of providing security protection for communication participants. Therefore, try to design a robust and efficient mutual authentication is meaningful and interesting.

Recently, numerous authentication schemes have been proposed for SIP [7-12]. In 2005, Yang et al.[15] proposed a Diffie-Hellman key exchange authentication scheme. However, both Kong [16] and Ring [17] found that Yang et al.'s scheme was vulnerable to replay attack. Later, Durlanik and Sogukpinar [18] also pointed out that the computational cost of Yang et al.'s scheme was very high and an enhanced authentication scheme was proposed by adopting Elliptic Curve Cryptography (ECC) which offered equivalent security with smaller key size as any other cryptosystem [19,20]. Unfortunately, Yoon et al.[21] found that Durlanik and Sogukpinar's scheme could not withstand the stolen verifier and off-line password guessing attacks. They then presented a secure ECC based authentication scheme for SIP to eliminate the flaws of Durlanik and Sogukpinar's scheme. Tsai [22] proposed an efficient authentication scheme only using hash functions and random numbers, which largely reduced the computation cost. However, Arshad and Ikram [23] showed that Tsai's scheme failed to achieve known-key secrecy and perfect forward secrecy while it was susceptible to off-line password guessing and stolen-verifier attacks. Subsequently, they presented an ECC based authenticated key agreement scheme and declared that the proposed scheme was immune to possible attacks.

This study concentrates on Arshad and Ikram's scheme. We find that Arshad and Ikram's scheme cannot protect against internal and masquerade attacks while not providing anonymity and update password phase. To remedy these weaknesses, we propose an improved scheme and maintain benefits of the original

scheme at the cost of increasing the computation consumptions slightly. By a careful security analysis and BAN logic [24] analysis of our scheme, we show that it is more secure than other related schemes.

The remainder of this paper is organized as follows. Section 2 introduces some notations and associated difficult problems based on the Elliptic Curve Diffie-Hellman (ECDH). The review and security analysis of Arshad et al.'s scheme are shown in Section 3 and Section 4, respectively. Section 5 shows our proposed scheme. Section 6 presents a security analysis of our scheme. The performance and functionality comparison among the proposed scheme and other related schemes are shown in Section 7. Section 8 is a brief conclusion.

2. Preliminaries

In this section, we show some notations and hard problems related with the ECC . Some notations used in this paper are shown in Table 1.

Table 1. Notations

Notation	Description
U , S	User and Server
ID_A	Identity of an entity A
PW_A	Password of an entity A
p_A	Secret key selected by A
s	Private key of S
Q_S	Public key selected of S
R_A	A random number selected by A
$F_s(\cdot)$	A trapdoor function
$h(\cdot)$	A one-way hash function
P	Generator point on the elliptic curve
$E_K[m]$	Encrypt the message m using the symmetric key K
$D_K[m]$	Decrypt the message m using the symmetric key K
$\oplus$	Exclusive-or operation
$\|\|$	Concatenation operation

2.1. Hard problems

1. Given points A, B over $E_p(a,b)$, the computational discrete logarithm (CDL) problem is to decide $m \in F_p^*$ from $B = mA$.
2. Given points mP, nP over $E_p(a,b)$, the computational Diffie-Hellman (CDH) problem is to compute mnP. Note that ECC is defined as the form of $E_p(a,b): y_2 = x_3 + ax + b(\text{mod } p)$ over a prime finite field F_p , where $a,b \in F_P$ and $4a^3 + 27b^2 \neq 0(\text{mod}p)$.
3. Given points P, mP over $E_p(a,b)$, the inverse computational Diffie-Hellman (ICDH) problem is to find $m^{-1}P$.

3. A review of Arshad and Ikram's scheme

In this section, we briefly review the Arshad and Ikram's scheme. There are two phases in Arshad and Ikram's scheme: registration and authentication.

3.1. Registration

1) U delivers his ID_U and password PW_U to S ;

2) S computes $HPW = h(ID_U \| PW_U)$, $HK_S = h(ID_U \| p_S)$ and $VPW = HPW \oplus HK_S$,where p_S is the secret key of S . Then, S stores $\{HPW, HK_S\}$ into his database.

3.2. Authentication and the session key establishment

1) U calculates $HPW = h(ID_U \| PW_U)$ and selects a random number R_U . Then, U computes $A = HPWR_U P$ and sends the request message $\{ID_U, A\}$ to S ;

2) When receiving the login message, S first extracts HPW from VPW and computes HPW^{-1} by Extended Euclidean Algorithm. Next, S generates a random number R_S and computes $B = R_S P$, the session key $SK_S = h(R_S R_U P)$ and $h_1 = h(SK_S \| B)$. Finally, S sends the challenge message $\{realm, B, h_1\}$ to U .

3) After receiving the message, U computes $SK_U = h(R_U B)$ and checks whether $h_1^{'} = h(SK_U \| B) \stackrel{?}{=} h_1$. If they are correct, U computes $h(ID_U \| realm \| SK_U)$ and sends the response message $\{ID_U, realm, h(ID_U \| realm \| SK_U)\}$ to S .

4) On receiving the message, S computes $h(ID_U \| realm \| SK_S)$ and checks whether it is equal to the received value. If they are equal, U and S share the session key SK . The process of authentication phase is shown in Figure 1.

4. Weaknesses of Arshad and Ikram's scheme

In this section, we show that Arshad and Ikram's scheme is vulnerable to internal and masquerade attacks while not providing anonymity and password changing phase. The following attacks are based on the assumptions that a malicious attacker C has

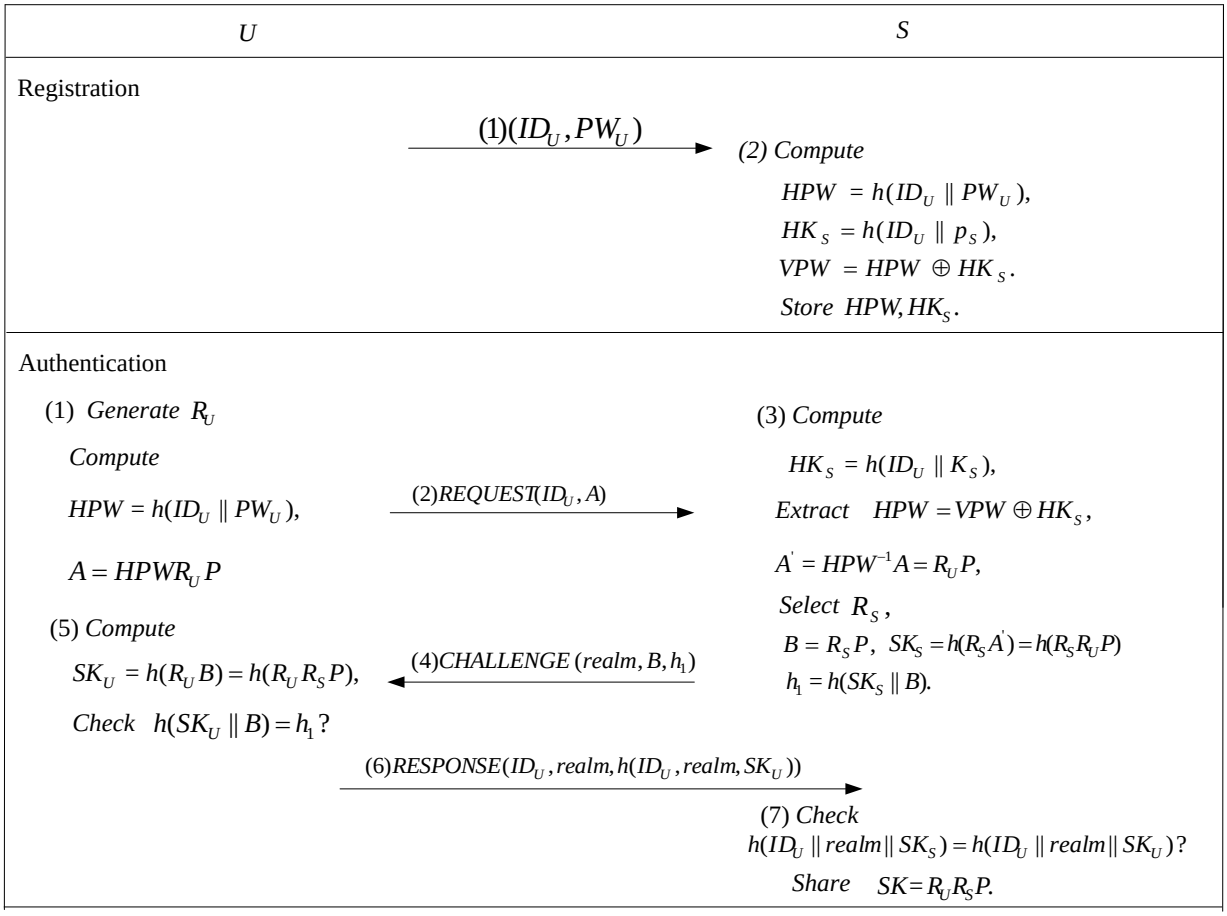

Figure 1. Authentication and the session key establishment phase of Arshad and Ikram's scheme

completely monitor over the communication channel connecting U and S in authentication and the session key establishment phase. So C can eavesdrop, modify, insert, or delete any message transmitted via public channel [25].

4.1. Anonymity

In Arshad and Ikram's scheme, U 's ID_U is exposed in public channel. Thus, any malicious attacker can intercept the message among the communication channel and easily trace who communicates with S .

4.2. Internal attack

In the registration phase of Arshad and Ikram's scheme, U 's plain-text password PW_U is directly revealed to S . Assume there is an inside malicious sever C who has known ID_U and PW_U . Next, he can firstly compute $h(ID_U \| PW_U)$ and then further launch intercepting attack to get the session key shared among any other users, the related service is provided by servers. Thus, Arshad and Ikram's scheme cannot withstand internal attack.

4.3. Masquerade attack

In Arshad and Ikram's scheme, after S receives the request message $\{ID_U, A\}$ from U , S does not verify whether the request message comes from the legal user U . Therefore, as described in the previous subsection, we assume U 's PW_U has been leaked. Moreover, the request message $\{ID_U, A\}$ has been eavesdropped by the attacker C . And then, C selects a random number PW_U and sends the forged request message $\{ID_U, A'\}$ to S , the session still continue in their scheme, where $A' = h(ID_U \| PW_U)R_U' P$. Finally, C who is masquerading as U and S will authenticate each other and agree on the common session key.

4.4. Lack of password update option

When U 's password is expired or leaked, U may wish to change PW_U ,for the sake of security. Moreover, it is a widely recommended security policy for highly secure applications that users' password should be updated or changed frequently. However, there is no such option in Arshad and Ikram's scheme.

5. Advanced scheme

In this section, we propose an improved mutual authentication scheme for SIP. Our proposed scheme not only overcomes weaknesses of Arshad and Ikram's scheme but also achieves mutual authentication and resists internal attack.

5.1. Registration

1) U chooses his password PW_U, his own secret key p_U. Then, U computes $PWD_U = h(PW_U \| p_U)$, $HID = h(ID_U \| PWD_U)$ and submits $\{ID_U, HID\}$ to S via a secure channel.

2) When receiving the message, S computes $EID = HID \oplus h(p_S)$ and stores EID in its database.

5.2. Mutual authentication and key agreement

1) U generates a random number R_U and calculates $T = R_U P$ $M = E_{R_S Q_S}[ID_U]$, $U = h(ID_U \| HID \| T)$. Then, U delivers the request message $\{M, T, U\}$ to S.

2) After receiving the message, S first decrypts M by using the symmetric key sT to derive ID_U and checks whether $h(ID_U \| (EID \oplus h(p_S)) \| T)$ is equal to the received U. If it holds, S generates a random number R_S and calculates $H_S = R_S P$, $SK = R_S T$, $Auth = h(SK \| HID \| T \| sT \| ID_U)$.

Finally, S sends the challenge message $\{realm, H_S, Auth\}$ to S.

3) On receiving the message, U computes $SK = R_U H_S$ and checks whether $h(SK \| h(ID_U \| PWD_U) \| R_U P \| R_U Q_S) \stackrel{?}{=} Auth$. If they are not correct, the session is terminated. Otherwise, U computes $V_U = h(SK \| ID_U \| H_S \| HID)$, and then sends the response message $\{realm, V_U\}$ to S.

4) Upon receiving the message, S verifies $h(SK \| HID \| R_S P \| ID_U) \stackrel{?}{=} V_U$. If they are not equal, S stops the session. Otherwise, S agrees on a common session key $SK = R_S T = R_U H_S$ with U.

5.3. Update the password

When U wants to change the password from PW_U to PW_U^{new}, he can finish this process with assistance from S.

1) U selects a random number R_U and p_U^{new}, then he submits $\{P = h(SK \| h(ID_U \| h(PW_U \| p_U)))$, $Q = h(SK \| R_U) \oplus h(ID_U \| h(PW^{new} \| p_U^{new})))$, $R_U\}$ to S.

2) S calculates $h(SK \| (EID \oplus h(p_S)))$ and validates whether it is equal to the received P. If it is equal, S computes $EID^{new} = h(p_S) \oplus h(R_U \| SK) \oplus Q$ and then replaces EID with EID^{new}.

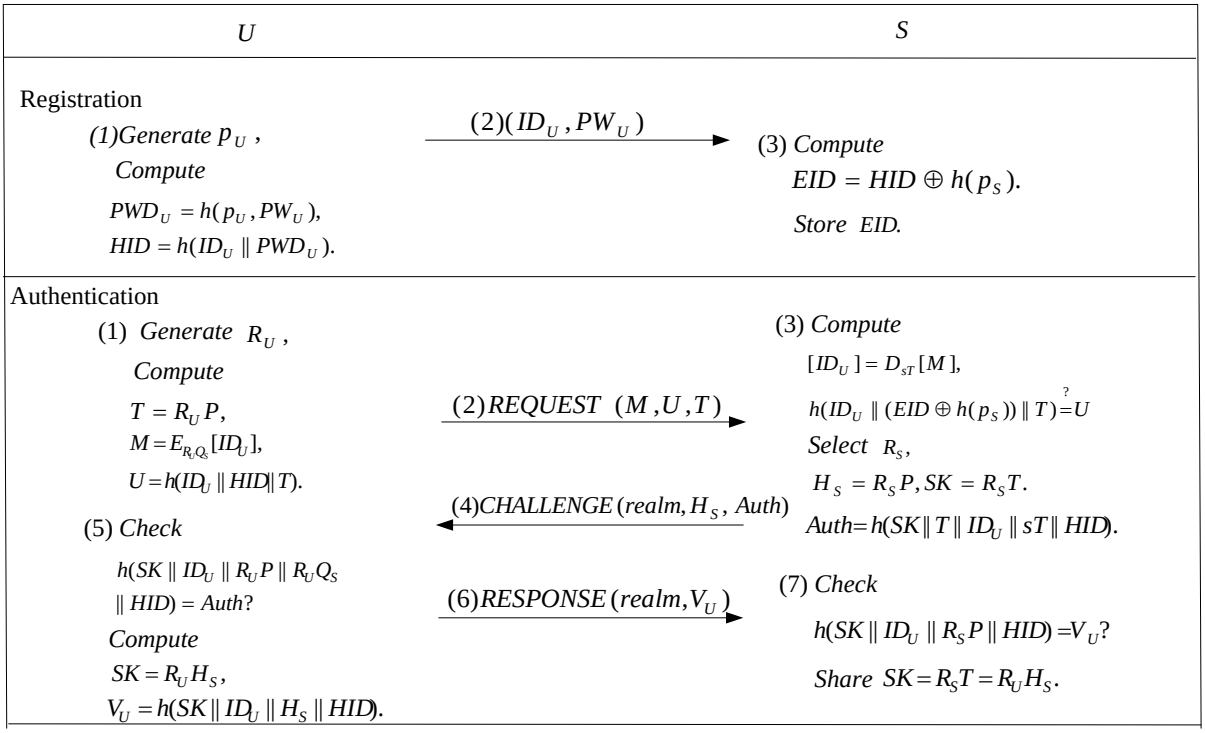

Figure 2. Authentication and the session key establishment phase of the proposed scheme

6. Security analysis

In this section, we first conduct discussion and a security analysis of the proposed scheme. Then, we apply Burrows-Abadi-Needham (BAN) logic [24] to demonstrate that the authentication process can correctly generate a session key between communicating entities. The following attacks are based on the assumptions that a malicious attacker C has completely monitor over the communication channel connecting U and S in mutual authentication and key agreement phase. So C can eavesdrop, modify, insert, or delete any message transmitted via public channel [25].

6.1. Anonymity

In our scheme, user's real identity ID_U is not directly revealed in an open channel. ID_U is protected by symmetric cryptography, where the symmetric key $R_U Q_S$ is related with user's random number and the server's public key. The legal server can gain the correct data by using his private key. Any third parties are not able to know which service is request by U.

6.2. Internal attack

In the registration phase, U submits $\{ID_U, HID\}$ instead of $\{ID_U, PW_U\}$, where $HID = h(ID_U \| h(PW_U) \| p_U)$. The sever S cannot retrieve the user's password because of the property of the hash function and secret information. Thus, C will be unable to plot internal attack successfully.

6.3. Mutual authentication

In our scheme, S authenticates U by verifying $h(ID_U \| (EID \oplus h(p_S)) \| T) \stackrel{?}{=} U$, $h(SK \| ID_U \| R_S P \| HID) \stackrel{?}{=} V_U$. U authenticates S by checking $h(SK \| ID_U \| R_U P \| R_U Q_S \| HID) \stackrel{?}{=} Auth$.

Thus, our scheme provides mutual authentication between U and S.

6.4 Masquerade attack

In our mutual authentication phase, when C tries to masquerade as a legal user, he cannot generate a proper message M since he lacks p_U and PW_U to compute the verifier HID. Moreover, it would not be feasible for C to attempt to modify the intercepted message V_U, because he cannot compute the correct session key lacking of two one time random numbers R_U and R_S which are based on the CDL problem. Besides, when C tries to masquerade as a legal server, he will be detected by the user because he cannot generate the correct message $Auth = h(SK \| ID_U \| T \| sT \| HID)$ for validation. R_U and R_S are generated by U and S, respectively. Thus, our proposed scheme can withstand the masquerade attack.

6.5. Verifier attack

Even though C acquires EID stored in S, he does not have sufficient information to calculate user's identity and password since they are hidden in a hash function with S 's secret key p_S. Therefore, our scheme is secure against verifier attack.

6.6. Replay attack

In our scheme, even if C initiates a parallel session to imitate legitimate user to login onto the server by resending the captured messages transmitted from U to S, he cannot be authenticated successfully by S. Since U generates a new random number R_U for each authentication request, the previous T is not equal to the new one. Therefore, the proposed scheme is secure against replay attack.

6.7. Perfect forward secrecy

Even though C can compromise all the passwords of communication entities, he cannot compromise the session key at all. In our scheme, $SK = R_S R_U P$ is generated by U and S, respectively. C cannot obtain R_S and R_U at the same time from $H_S = R_S P$, $T = R_U P$ based on the security of CDL problem. Thus, our scheme can achieve perfect forward secrecy.

7. Verifying authentication scheme with BAN logic

We introduce some notations and logical postulates of BAN logic that we will use in our scheme.

1. BAN logical postulates

a. Message-meaning rule: $\dfrac{A \mid\equiv A \leftrightarrow B, A \lhd\!<\!\!<_K M >_K}{A \mid\equiv B \mid\sim M}$:
if A trusts that A and B share K, and sees M encrypted with K, A then trusts B once said M.

b. Fresh conjuncatenation rule: $\dfrac{A \mid\equiv \#(M)}{A \mid\equiv \#(M, N)}$: if A trusts freshness of M, A then trusts freshness of (M, N).

c. Belief rule: $\dfrac{A \mid\equiv M, A \mid\equiv N}{A \mid\equiv (M, N)}$: if A trusts M and A trusts N, then A trusts M and N.

d. Nonce-verification rule: $\dfrac{A \mid\equiv \#M, A \mid\equiv B \mid\sim M}{A \mid\equiv B \mid\equiv M}$: if A trusts that the freshness of M and that B once said M, then A trusts that B trusts M.

Table 2. BAN logic notations

Notation	Description
$A \mid\equiv X$	A trusts X
$U \overset{K}{\leftrightarrow} S$	Share a key K between user and sever
$\#X$	X is fresh
$A \lhd X$	A sees X
$A \mid\sim X$	A said X
(X,Y)	X or Y is one part of (X,Y)
$< X >_K$	X is encrypted with K
$\{X\}_K$	X is hashed with K

Table 3. Functionality comparison

	Ours	[23]	[22]	[12]	[11]	[10]
Provide anonymity	Yes	No	No	Yes	Yes	Yes
Provide mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes
Provide perfect forward secrecy	Yes	Yes	-	-	Yes	Yes
Password changing phase	Yes	No	No	Yes	Yes	No
Resist insider attack	Yes	No	No	Yes	Yes	Yes
Resist masquerade attack	Yes	No	No	Yes	Yes	Yes
Resist replay attack	Yes	Yes	No	Yes	Yes	-
Resist verifier attack	Yes	No	No	-	-	Yes

e. Jurisdiction rule: $\dfrac{A \mid\equiv B \Rightarrow M, A \mid\equiv B \mid\equiv M}{A \mid\equiv M}$:

f. if A trusts that B has jurisdiction over M and A trusts B on the fact of M, A then trusts M.

2. Idealized scheme

$U \to S \quad : \quad < ID_U >_{U \overset{R_U Q_S}{\leftrightarrow} S} \quad , \quad \{ID_U, T\}_{U \overset{HID}{\leftrightarrow} S} \quad ,$

$\{U \overset{SK}{\leftrightarrow} S, H_S, ID_U\}_{U \overset{HID}{\leftrightarrow} S}, T$

$S \to U : \{U \overset{SK}{\leftrightarrow} S, R_U P, ID_U, sT\}_{U \overset{HID}{\leftrightarrow} S}, H_S$

3. Establishment of security goals

$goal_1 : U \mid\equiv S \mid\equiv U \overset{SK}{\leftrightarrow} S$

$goal_2 : U \mid\equiv U \overset{SK}{\leftrightarrow} S$

$goal_3 : S \mid\equiv U \mid\equiv U \overset{SK}{\leftrightarrow} S$

$goal_4 : S \mid\equiv U \overset{SK}{\leftrightarrow} S$

4. Initiative premises

$p_1 : U \equiv \#R$

$p_2 : S \mid\equiv \#R_S$

$p_3 : U \mid\equiv U \overset{HID}{\leftrightarrow} S$

$p_4 : S \mid\equiv U \overset{HID}{\leftrightarrow} S$

$p_5 : S \mid\equiv U \Rightarrow (U \overset{R_U Q_S}{\leftrightarrow} S)$

$p_6 : U \mid\equiv S \Rightarrow (U \overset{R_U Q_S}{\leftrightarrow} S)$

$p_7 : U \mid\equiv S \Rightarrow (U \overset{SK}{\leftrightarrow} S)$

$p_8 : S \mid\equiv U \Rightarrow (U \overset{SK}{\leftrightarrow} S)$

5. Scheme analysis

a_1:Since p_3 and

$U \lhd \{U \overset{SK}{\leftrightarrow} S, R_U P, ID_U, sT\}_{U \overset{HID}{\leftrightarrow} S}$,

through the message-meaning rule, we obtain:

$U \mid\equiv S \mid\sim (U \overset{SK}{\leftrightarrow} S, R_U P, ID_U, sT)$.

a_2 : Since p_1 and a_1, through the fresh conjuncatenation rule and nonce-verification rule, we obtain: $U \mid\equiv S \mid\sim (U \overset{SK}{\leftrightarrow} S, ID_U, sT)$

a_3: Since a_2, through the belief rule, we obtain: $U \mid\equiv S \mid\equiv U \overset{SK}{\leftrightarrow} S(goal_1), U \mid\equiv S \mid\equiv U \overset{sT}{\leftrightarrow} S$.

$goal_2$: Since $goal_1$ and p_7, through the jurisdiction rule, we obtain: $U \mid\equiv U \overset{SK}{\leftrightarrow} S$.

a_4 :Since $S \lhd \{U \overset{SK}{\leftrightarrow} S, ID_U, H_S\}_{U \overset{HID}{\leftrightarrow} S}$ and p_4, through the message-meaning rule, we obtain: $S \mid\equiv U \mid\sim (U \overset{SK}{\leftrightarrow} S, H_S, ID_U)$.

a_5 : Since a_4 and p_2, through the fresh conjuncatenation rule and nonce-verification rule, we obtain:

$S \mid\equiv U \mid\equiv (U \overset{SK}{\leftrightarrow} S, ID_U)$.

a_6: Since a_5, through the belief rule, we obtain: $S \mid\equiv U \mid\equiv U \overset{SK}{\leftrightarrow} S(goal_3)$, $S \mid\equiv U \mid\equiv ID_U$.

$goal_4$: Since p_8 and $goal_3$, through the jurisdiction rule, we obtain: $S \mid\equiv U \overset{SK}{\leftrightarrow} S$.

Table 4. Comparison of computational costs

	Ours	Arshad and Ikram [23]	Tsai [22]	Kumari et al.'s scheme [12]	Chaudhry et al's scheme [11]	Chaudhry et al's scheme [10]
U	$3H+3PM+1S$	$3H+3PM$	$2H$	$5H+1PA+3PM$	$5H+3PM$	$5H+1PA+3PM$
S	$4H+3PM+1S$	$4H+3PM$	$3H$	$5H+2PM$	$3H+1PM$	$5H+3PM+2S$
Total	$7H+6PM+2S$	$7H+5PM$	$5H$	$10H+1PA+5PM$	$8H+4PM$	$10H+1PA+6PM+2S$

8. Performance and security properties comparison

In this section, we compare the functionality and performance of our scheme with Chaudhry et al's scheme [10,11], Kumari et al.'s scheme [12], Tsai's scheme [22] , Arshad and Ikram's scheme [23]. All comparisons are described as Tables 3 and 4. From Table 3, we can see that the proposed scheme can provide proper user anonymity and password changing phase while preventing insider, masquerade, and verifier attacks, where Tsai's [22] and Arshad and Ikram's schemes[23] fail to cope with, Chaudhry et al's. scheme [10] cannot provide password change phase, both of Chaudhry et al.'s scheme [11] and Kumari et al.'s scheme [12] fail to consider verifier attack. The computation cost of these schemes is shown in Table 4, where H , PM , PA, and S denote a hash function operation, an elliptic curve scalar point multiplication operation, an elliptic curve point addition operation, a symmetrical cryptography operation and exclusive-OR operations separately. From Table 4, we can see that Tsai's scheme [22] has better performance than Chaudhry et al.'s scheme [11], Kumari et al.'s scheme [12], Arshad and Ikram's scheme [23], and the proposed scheme, but Chaudhry et al.'s scheme [10] consumes a slightly higher than our scheme. In a word, the proposed scheme is more secure and has many excellent features compared with these related schemes.

9. Conclusion

In this paper, we have presented a security analysis of the Arshad and Ikram's scheme and shown that the scheme is vulnerable to internal, masquerade attacks and can not provide anonymity and password changing phase. An advanced scheme is proposed that inherits the merits of the Arshad and Ikram's scheme and resists the aforementioned attacks with a slight higher computation cost than others. Finally, in comparison with the previously proposed schemes on security and performance, our scheme is efficient and more secure than other related schemes.

Acknowledgments

The authors would like to thank all the anonymous reviewers for their helpful advice. This paper is supported by the National Natural Science Foundation of China (Grant Nos. 61472045, 61573067), the Beijing Natural Science Foundation (Grant No. 4142016), BUPT Excellent Ph.D. Students Foundation (Grant No. CX2015310), and the Asia Foresight Program under NSFC Grant (Grant No. 61411146001).

References

[1] **S. Salsano, L. Veltri, D. Papalilo.** SIP security issues: the SIP authentication procedure and its processing load. *IEEE Network,* 2002, Vol. 16, No. 6, 38-44.

[2] **J. Arkko, G. Camarillo, T. Haukka, S. Sen, V. Torvinen.** Security mechanism agreement for SIP sessions. *IETF Internet Draft,* 2002, Jun 3.

[3] **M. Thomas.** SIP Security Requirements. *IETF Internet Draft,* 2001, November.

[4] **J. L. Tsai, N. W. Lo, T. C Wu.** Novel anonymous authentication scheme using smart cards. *IEEE Transactions on Industrial Informatics,* 2013, Vol. 9, No. 4, 2004-2013.

[5] **M. Heydari, S. M. S. Sadough, M. S. Farash, S. A. Chaudhry, K. Mahmood**. An efficient password-based authenticated key exchange protocol with provable security for mobile client-client networks. *Wireless Personal Communications,* 2016, Vol. 88, No. 2, 337-356.

[6] **S. A. Chaudhry, M. S. Farash, H. Naqvi, SK. H. IsIam, T. Shon.** A robust and efficient privacy aware handover authentication scheme for wireless networks. *Wireless Personal Communications,* 2015, 1-25. DOI: 10.1007/s11277-015-3139-y

[7] **S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, M. K. Khan.** An enhanced privacy preserving remote user authentication scheme with provable security. *Security and Communication Networks,* 2015, Vol. 8, No. 18, 3782-3795.

[8] **H. H. Kilinc, T. Yanik.** A survey of SIP authentication and key agreement schemes. *IEEE Communications Surveys & Tutorials,* 2014, Vol. 16, No. 2, 1005-1023.

[9] **H. L. Yeh, T. H. Chen, W. K. Shih.** Robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Computer Standards & Interfaces,* 2014, Vol. 36, No. 2, 397-402.

[10] **S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, M. U. Hassan.** An improved and provably secure privacy preserving authentication protocol for SIP. *Peer-to-Peer Networking and Applications*, 2015, 1-15. DOI: 10.1007/s12083-015-0400-9

[11] **S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, M. S. Farash.** Cryptanalysis and improvement of an Improved two factor authentication protocol for telecare medical information systems. *Journal of Medical Systems*, 2015, Vol. 39, No. 6, 1-11.

[12] **S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, M. K. Khan.** An improved smart card based authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Applications*, 2015, 1-14. DOI: 10.1007/s12083-015-0409-0

[13] **H. Tu, N. Kumar, N. Chilamkurti, S. Rho**. An improved authentication protocol for session initiation protocol using smart card. *Peer-to-Peer Networking and Applications*, 2015, Vol. 8, No. 5, 903-910.

[14] **L. P. Zhang, S. Y. Tang, Z. H. Cai.** Robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications. *IET Communications*, 2014, Vol. 8, No.1, 83-91.

[15] **C. C. Yang, R. C. Wang, W. T. Liu.** Secure authentication scheme for session initiation protocol. *Computers & Security*, 2005, Vol. 24, No. 5, 381-386.

[16] **L. Kong, V. A. Balasubramaniyan, M. Ahamad.** A lightweight scheme for securely and reliably locating SIP users. In: *2006 IEEE Workshop on VoIP Management and Security*, 2006, pp. 9-17.

[17] **J. W. Ring, K. K. R Cho, E. Foo, M. H. Looi.** A new authentication mechanism and key agreement protocol for SIP using identity based cryptography. *Asia Pacific Inforamtion Technology Security Conference*, 2006, pp. 61-72.

[18] **A. Durlanik, I. Sogukpinar.** SIP authentication scheme using ECDH. In: *Proceedings of World Academy of Science Engineering and Technology*, 2005, Vol. 8, pp. 350-353.

[19] **A. J. Menezes, P. C. Van Oorschot, S. Vanstone.** Handbook of applied cryptography. *CRC Press New York*, 1997.

[20] **S. A. Vanstone.** Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments. *Information Security Technical Report*, 1997, Vol. 2, No. 2, 78-87.

[21] **E. J. Yoon, K. Y. Yoo.** Cryptanalysis of DS-SIP authentication scheme using ECDH. *In: 3rd International Conference on New Trends in Information and Service Science*, 2009, pp. 642-647.

[22] **J. L. Tsai.** Efficient nonce-based authentication scheme for session initiation protocol. *International Journal of Network Security*, 2009, Vol. 9, No.1, 12-16.

[23] **R. Arshad, N. Ikram.** Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. *Multimedia Tools and Applications*, 2013, Vol. 66, No. 2, 165-178.

[24] **M. Burrow, M. Abadi, R. M. Needham.** A logic of authentication. *ACM Transactions on Computer Systems*, 1990, Vol. 8, No. 1, 18-36.

[25] **L. Lamport.** Password authentication with insecure communication. *Communications of the ACM*, 1981, Vol. 24, No. 11, 770-772.

Received October 2015.